FedRAMP CIGIE

Matt Goodrich, FedRAMP Director
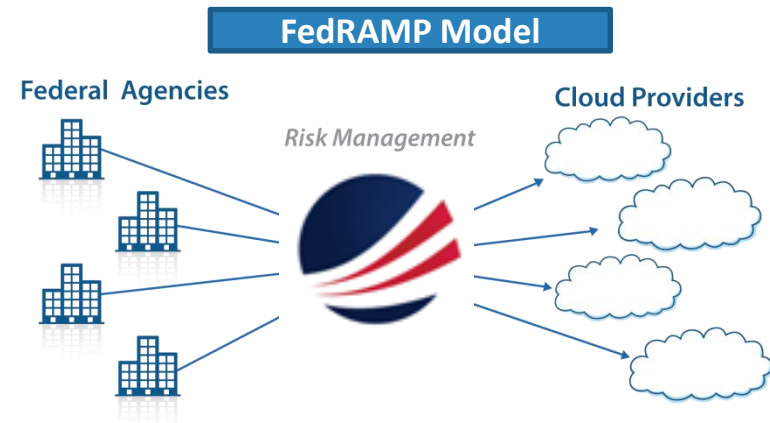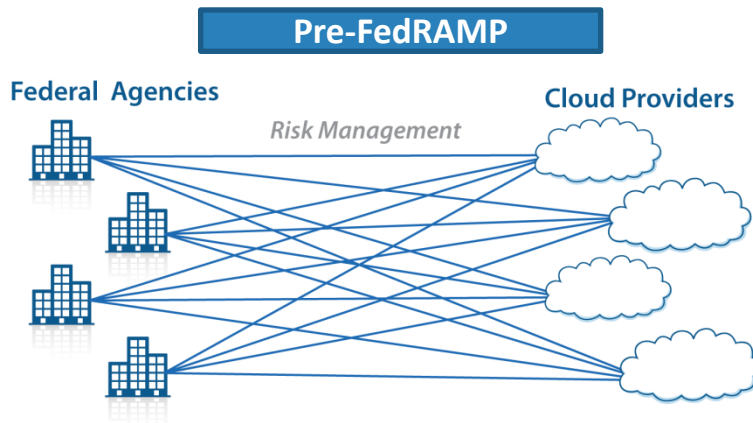
January 28, 2014

FedRAMP Overview
Ensuring Secure Cloud Computing

- FedRAMP was established via OMB Memo in December 2012.
- FedRAMP is the first government-wide security authorization program for FISMA – mandatory for all agencies and all cloud services
- FedRAMP's framework is being modeled in other government security programs (mobile, data) and by other countries (Canada, UK, EU, China)
- FedRAMP's focus is to ensure the rigorous security standards of FISMA are applied while introducing efficiencies to the process for cloud systems, key of which is re-use
- Conservative cost estimates for FedRAMP is $40M for the government alone

FedRAMP Overview
Current CSP Statistics

Authorizations

- JAB P-ATOs - 15
  - Includes services from IBM, Microsoft, Akamai, HP, LMCO
- Agency ATOs - 12
  - Includes Amazon, AINs, USDA, Micropact, Salesforce
- CSP Supplied - 2

In Process CSPs

- JAB P-ATO – 14
  - Includes services from Dell, SecureKey, Oracle, Amazon, Microsoft, IT-CNP, IBM
- Agency ATOs – 24
  - Includes Microsoft, Google, Adobe, IBM, Oracle, Verizon
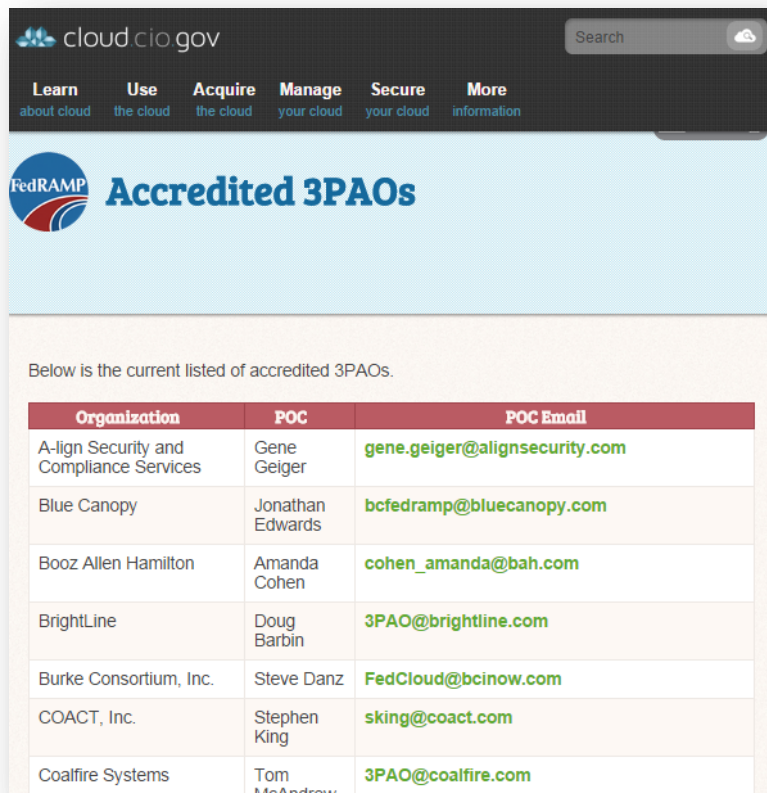
Cloud Auditor Accreditation (3PAO Program)

- First program (Federal or private) to accredit cloud auditors
- 31 organizations accredited to date
  - Including KPMG, Ernst & Young, Veris, Booz Allen Hamilton
  - ~60% are small businesses
  - One government agency (USDA ESC)
- Privatized in Nov 2013 with A2LA
  - Seeing our first 3PAOs authorized through A2LA
  - Includes new 3PAOs and re-accreditation of existing 3PAOs

FedRAMP PMO 3PAO Program Oversight

- Define and update 3PAO requirements – ISO 17020 and FISMA
- Use a conformity assessment approach
- Can revoke accreditation at any time
- Requires 3PAO to agree to adhere to requirements for rigor and independence
- Access to evidence and reports created by A2LA

cloud.cio.gov

| Learn | Use | Acquire | Manage | Secure | More |
| about cloud | the cloud | the cloud | your cloud | your cloud | information |

FedRAMP Accredited 3PAOs

Below is the current listed of accredited 3PAOs.

Organization	POC	POC Email
A-lign Security and Compliance Services	Gene Geiger	gene.geiger@alignsecurity.com
Blue Canopy	Jonathan Edwards	bcfedramp@bluecanopy.com
Booz Allen Hamilton	Amanda Cohen	cohen_amanda@bah.com
BrightLine	Doug Barbin	3PAO@brightline.com
Burke Consortium, Inc.	Steve Danz	FedCloud@bcinow.com
COACT, Inc.	Stephen King	sking@coact.com
Coalfire Systems	Tom McAndrew	3PAO@coalfire.com

FedRAMP Forward: 2 Year Priorities

FedRAMP Forward
Two Year Priorities

FedRAMP Forward

- Plan addresses prioritized activities for deliberate, and effective growth and success
- Addresses key program issues with a roadmap of regular outputs to keep stakeholders engaged and informed
- Primary objective to significantly increase agency role in FedRAMP ATOs and compliance while ensuring JAB focuses on highest impact ATOs

Key Outcomes:

- Accurate baseline metrics beyond PortfolioStat
- Training modules for FedRAMP
- FedRAMP agency working groups
- Automation requirements to increase efficiency
- Re-use of other industry standards within FedRAMP
- FedRAMP overlays that allow for compliance with other IT initiatives like TIC, IPv6, HSPD-12
- Creation of a high baseline

FedRAMP Forward
Increase Stakeholder Engagement

OBJECTIVE 1: INCREASE NUMBER OF AGENCIES IMPLEMENTING FEDRAMP

Establish Baseline Metrics, Implementation Guidance	Best Practices Reference Guide	Provide Agencies Implementation Support Options
6 months	12 months	18 months

OBJECTIVE 2: INCREASE CROSS-AGENCY COLLABORATION

Create Multi-Agency SAF WG Methodology	Launch Multi-Agency Security Assessment Framework Working Groups	Transition ConMon of low use P-ATOs to Agency WGs
6 months	12 months	18 months	24 months

OBJECTIVE 3: INCREASE UNDERSTANDING OF FEDRAMP

Re-Launch FedRAMP.gov, Develop Online Training, Program	Update Training Program With Modules Targeted for Procurement Officials and Program Managers	Ongong updates to guidance documents
6 months	12 months	18 months	24months

FedRAMP Forward
Improve Efficiencies

OBJECTIVE 4: ENHANCE CONSISTENCY & QUALITY OF 3PAO ASSESSMENTS & DELIVERABLES

Develop and Publish Updated 3PAO Requirements	Develop Targeted 3PAO Training,
6 months	12 months
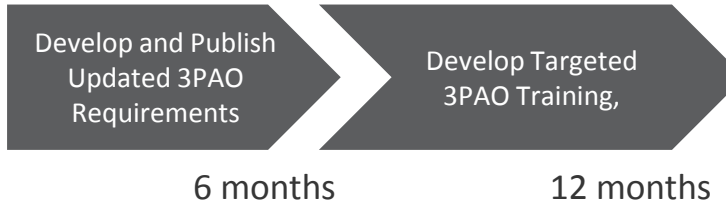
OBJECTIVE 5: ESTABLISH A FLEXIBLE FRAMEWORK FOR DATA & WORKFLOW MANAGEMENT

Identify Automation Capabilities	Conduct Industry Day	Draft Requirements	Finalize Requirements
6 months	12 months	18 months	24 months

OBJECTIVE 6: RE-USE INDUSTRY STANDARDS

Draft Requirements for Industry Standard Re-Use	Map Evidence Re-Use for 1 Industry Standard	Complete Pilot of Evidence Re-Use	Publish Additional Industry Standard Mappings
6 months	12 months	18 months	24 months

FedRAMP Forward
Continue to Adapt

OBJECTIVE 7: EVOLVE CONTINUOUS MONITORING

Publish ConMon Roadmap, Key Indicators For Risk Review	Publish Guidelines For Correlating ConMon Data	Automate and Correlate ConMon Across 2 Agency and 2 P-ATO	Automate and Correlate All P-ATO and Participating Agency ConMon
6 months	12 months	18 months	24 months

OBJECTIVE 8: ESTABLISH ADDITIONAL BASELINES

Draft High Baseline for Public Comment	Finalize High Baseline	Identify Additional Agency baselines	Draft Additional Baselines Based Upon Agency Needs
6 months	12 months	18 months	24 months

OBJECTIVE 9: ENHANCE INTEGRATION W CYBER INITIATIVES & CONTRIBUTE TO POLICY REFORM

Draft Initial FedRAMP Overlay to IT Policies	Initial Assessment Using Overlay of IT Policies	Finalize Framework For IT Policies Overlays	Develop Two (2) Additional IT Policies Overlays
6 months	12 months	18 months	24 months
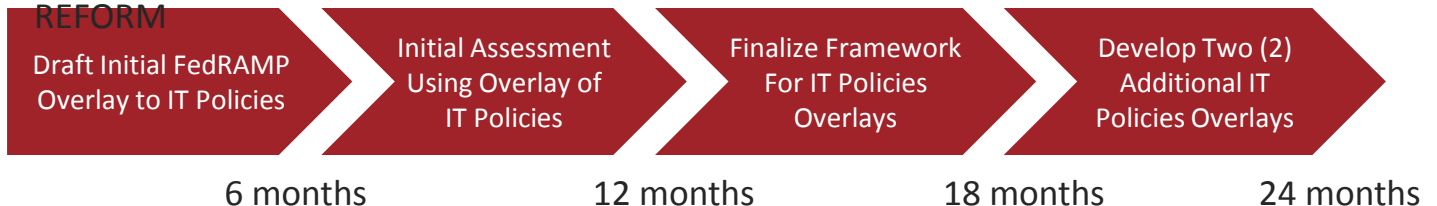
FedRAMP Guidance Updates

FedRAMP Development Update
Procurement Guidance

- OMB's FedRAMP Memo requires agencies to enforce FedRAMP via contractual provisions.

- Agencies are implementing FedRAMP via contractual provisions inconsistently and in ways that are overly restrictive.

- Agencies need more directed, specific, and authoritative guidance on how to appropriately include FedRAMP in their contracts.

- Working with OMB to develop joint OFPP and eGov guidance to agencies.

  – USG should foster a competitive marketplace of cloud providers - both new and established

  – Agencies must be willing to undertake authorizations as with any FISMA system – cloud and non-cloud